Процессы формирования и проверки электронной цифровой подписи на эллиптических кривых.. **6.** *A. Menezes, P. Oorschot, S. Vanstone "Handbook of Applied Cryptography", CRC Press, 1997, 780 с.*

УДК 681.3.06

ОЦЕНКА ВЕРОЯТНОСТИ ПЕРЕКРЫТИЯ ШИФРА В РЕЖИМЕ СЧЕТЧИКА

Юрий Горбенко, Денис Пономарев
Харьковский национальный университет радиоэлектроники

Аннотация: **Рассматривается и решается проблема расчета и обоснования срока действия ключей поточного шифра или блочного шифра, используемого в режиме гаммирования. Произведена оценка вероятностей перекрытия шифра с использованием наиболее распространенных длин ключа.**
Summary: **The problem of calculating and estimation key validity time of stream cipher and block symmetric cipher in a counter mode has been considered and solved. The probability of overlapping estimation has been made for the most common key lengths.**
Ключевые слова: **Информационная безопасность, вероятность перекрытия шифра, поточный шифр, режим счетчика.**

Введение

Алгоритмы шифрования играют жизненно важную роль при защите таких данных, как медицинская и финансовая информация, уникальные персональные идентификационные номера (PIN) и т. д. Однако в последнее время возникает необходимость проверки качества функционирования шифров в некоторых режимах. Даная работа имеет целью анализ наиболее распространенных в настоящее время блочно симметричных криптоалгоритмов и оценка перекрытия таких шифров в режиме счетчика.

I Вероятность перекрытия шифра

Пускай вероятность перекрытия шифра равна $P_{пш}$. Тогда, исходя из того, что вероятности перекрытия и вероятность обратного этому события составляют полную группу событий, получаем: $P_{пш}+P_{оп}=1$. Вероятность $P_{оп}$ можно выразить как

$$P_{оп} = n_{оп}/n_{\Sigma}. \quad (1)$$

Тут $n_{оп}$ – число размещений n сообщений на периоде L без перекрытия за n обращений, а n_{Σ} является общим числом гамм, сформированных для n сообщений. При каждом обращении к алгоритму формирования гаммы шифрующей существует L вариантов выбора. Поскольку все обращения являются случайными, то на n обращениях

$$n_{\Sigma} = \mathrm{L}^n. \quad (2)$$

За n обращений $n_{оп}$ можно описать, учтя, что при первом обращении существует $n_1=n$ вариантов выбора гамм. При втором и последующих обращениях соответственно имеется n–1, n–2 ... и т. д. вариантов выбора отрезков. Таким образом, всего можем выбрать:

$$n_{оп}=(n-1)! \quad (3)$$

Далее поскольку отрезки не перекрываются, то расстояния между ними будут $x_1, x_2, \ldots, x_n \geq 0$ и таких расстояний будет n. Значит, справедливым будет следующее выражение

$$\sum_{i=1}^{n} x_i + \sum_{i=1}^{n} l_i = L. \quad (4)$$

Из этого выражения следует, что число свободных для размещения позиций в периоде будет равно

$$\sum_{i=1}^{n} x_i = L - \sum_{i=1}^{n} l_i = L - Z, \quad (5)$$

где $Z=nl_M$ – произведение длин сообщений l_M на их число n.

Определить число разных расстановок $n-1$ перегородок между $L-Z$, т. е. число способов размещения n предметов по $L-Z$ ящикам [1, 2], можно по следующей формуле

$$C_{L-Z+r-1}^{r-1}. \quad (6)$$

Далее, исходя из [3] сведем все вышестоящие составляющие вероятности неперекрытия шифра воедино, и учтя при этом, что с вероятностью перекрытия шифра они составляют полную группу событий, можем получить, что вероятность возникновения перекрытия для шифра может быть рассчитана как

$$P_{пш} = 1 - \frac{(n-1)!\,C_{n-1}^{L-Z+n-1}}{L^{n-1}}. \tag{7}$$

II Математические методы упрощения эталонной формулы оценки вероятности перекрытия шифра в режиме счетчика

При подсчете напрямую по формуле (7) требуется ЭВМ сверхвысокой вычислительной мощности, поэтому целесообразно произвести упрощение в соответствии с формулами математической статистики.

Существует несколько математических методов ее упрощения.

Первый метод.

Развернем формулу (7) в виде

$$P_{пш} = 1 - \frac{(n-1)!(L-Z+n-1)!}{(n-1)!(L-Z)!L^{n-1}} \tag{8}$$

и, сократив $(n-1)!$, получим

$$P_{пш} = 1 - \frac{(L-Z+n-1)!}{(L-Z)!L^{n-1}}. \tag{9}$$

Непосредственное вычисление вероятностей по формуле (9) представляет большие трудности, так как при этом определение биномиальных коэффициентов связанно с вычислением факториалов при больших аргументах. Величину факториала можно получить с достаточной точностью, если применить асимптотическую формулу Стирлинга [4]:

$$m! \approx \sqrt{2\pi m}\, m^m e^{-m}. \tag{10}$$

Заметим, что даже в худшем случае при $m = 1$, формула (10) дает относительную ошибку всего в 8%, а при $m = 100$ эта ошибка уменьшается до 0,08%. При произвольном m точное значение $m!$ отличается от асимптотического, вычисленного согласно (10), только множителем e^{ε_m}, причем $0 < \varepsilon_m < 1/12m$. Последнее позволяет достаточно точно оценить погрешность вычислений [5, 6].

Применив формулу (10), получим:

$$\begin{gathered}(L-Z+n-1)! \approx \sqrt{2\pi}(L-Z+n-1)^{(L-Z+n-\frac{1}{2})} \exp\{-(L-Z+n-1)\}, \\ (L-Z)! \approx \sqrt{2\pi}(L-Z)^{(L-Z+\frac{1}{2})} \exp\{-(L-Z)\}.\end{gathered} \tag{11}$$

Подставив в (9) находим:

$$\begin{aligned} P_{нш} &= 1 - \frac{(L-Z+n-1)^{(L-Z+n-\frac{1}{2})} \exp\{-(L-Z+n-1)\}}{(L-Z)^{(L-Z+\frac{1}{2})} \exp\{-(L-Z)\}L^{n-1}} = \\ &= 1 - \frac{(L-Z+n-1)^{(L-Z+n-\frac{1}{2})}}{(L-Z)^{(L-Z+\frac{1}{2})} L^{n-1}} \exp\{-n+1\} = \\ &= 1 - \frac{(L-Z)^{(L-Z+n-\frac{1}{2})}\left[1+\frac{n-1}{L-Z}\right]^{(L-Z+n-\frac{1}{2})}}{(L-Z)^{(L-Z+\frac{1}{2})} L^{n-1}} \exp\{-n+1\} = \\ &= 1 - \exp\{-n+1\}\frac{(L-Z)^{(n-1)}}{L^{n-1}}\left[1+\frac{n-1}{L-Z}\right]^{(L-Z+n-\frac{1}{2})}. \end{aligned} \tag{12}$$

Если справедливо ограничение для L, что его значение больше Z в 10 и более раз, т. е. $n << L - Z$, то, применяя бином Ньютона, получаем:

$$P_{нш} = 1 - \exp\{-n+1\}\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(L-Z+n-\frac{1}{2})} = \\ = 1 - \exp\{-n+1\}\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(L-Z)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}. \quad (13)$$

Асимптотически справедливо $\lim_{x\to\infty}(1-\frac{\gamma}{x})^x = e^{\gamma}$, и в нашем случае $\left[1+\frac{n-1}{L-Z}\right]^{(L-Z)} \to \exp\{n-1\}$ можно аппроксимировать. Это приводит к следующему соотношению

$$P_{нш} = 1 - \exp\{-n+1\}\exp\{n-1\}\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}.$$

Окончательно получаем:

$$P_{нш} = 1 - \left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})} \quad (14)$$

Аппроксимируя, можем получить:

$$P_{нш} \le 1 - \left[1-\frac{(n-1)Z}{L}\right] \cong \frac{(n-1)nl_m}{L}. \quad (15)$$

Однако данная аппроксимация является значительно менее точной и целесообразнее пользоваться формулой (14).

Второй метод.

Разделим обе части формулы (8) на $(L - Z)!$

$$P_{пш} = 1 - \frac{(L-Z+n-1)(L-Z+n-2)...(L-Z+1)}{L^{n-1}}. \quad (16)$$

Поскольку

$$(L-Z+n-1)(L-Z+n-2)...(L-Z+1) > (L-Z)^{n-1}, \quad (17)$$

то отсюда (т. к. все новые члены меньш $L - Z$) следует

$$P_{пш} < 1 - \frac{(L-Z)^{n-1}}{L^{n-1}} = 1 - \left(1-\frac{Z}{L}\right)^{n-1}. \quad (18)$$

Если $Z/L<<1$, то по биному Ньютона $(1-\alpha)^{\beta} \cong 1-\beta\alpha$

$$P_{пш} = 1 - \left(1-(n-1)\frac{Z}{L}\right), \quad (19)$$

и, т. к. $Z = l_{m*}n$, и $n>>1$, то получим

$$P_{пш} = (n-1)\frac{Z}{L} = \frac{n^2 l_m}{L}. \quad (20)$$

Из формулы (20) можно вывести формулу для приближенного вычисления количества ключей для заданного интервала последовательности при заданной вероятности совпадения ключей:

$$n \ge \sqrt{\frac{P_{пш}L}{l_m}}. \quad (21)$$

При условии кратности $P_{пш}=10^{2b}$ формула оценки принимает следующий вид:

$$n \ge 10^b\sqrt{\frac{L}{l_m}}. \quad (22)$$

Практически то же самое можно получить, используя в формуле (14) аппроксимацию бинома Ньютона $(1-\alpha)^{\beta} \cong 1-\beta\alpha$. Тогда при $P_{нш} << 1$ находим

$$P_{нш} = \frac{nl_M}{L}(n-1) - (n-0.5)\left[\frac{n-1}{L-nl_M}\right] \tag{23}$$

уравнение относительно n при известных параметрах $P_{нш}$, l_M и L.

Это уравнение легко приводится к кубическому относительно n уравнению

$$P_{пш}L - nl_M P_{пш} - n^2(l_M - 1) + n^3\frac{l_M^2}{L} = 0 \tag{24}$$

и в случае пренебрежения кубическим членом и при $n>>1$ можно легко прийти к приведенному выше решению (21).

III Оценка погрешностей вычисления

Однако, несмотря на то, что приведенные математические преобразования позволяют достаточно точно оценить величину вероятности перекрытия шифра для больших значений как периода, так и выборки, они также вносят определенную погрешность в процесс вычисления. Возникает необходимость оценки абсолютной или относительной погрешностей, полученных при расчете при разных значениях аргумента. Абсолютной погрешностью [6] числа a называется разница $x–a$, где a – исходное число, которое рассматривается как приближенное значение некоторой величины, точное значение которой x. Относительной же погрешностью числа a называется отношение вида:

$$\frac{x-a}{a} = \delta(a). \tag{25}$$

Число $\delta(a)$ такое, что:

$$\left|\frac{x-a}{a}\right| \le \delta(a) \tag{26}$$

называется границей относительной погрешности.

На первом этапе оценим погрешность, полученную в результате применения асимптотической формулы Стирлинга (10). Для абсолютной погрешности имеем:

$$\left|\Delta_a\right| = \left|\sqrt{2\pi m}m^m e^{-m}e^{\theta(m)} - \sqrt{2\pi m}m^m e^{-m}\right| = \sqrt{2\pi m}m^m e^{-m}\left|e^{\theta(m)} - 1\right| \tag{27}$$

Относительная погрешность

$$\delta(a) = \frac{\Delta_a}{\sqrt{2\pi m}m^m e^{-m}} = \frac{\sqrt{2\pi m}m^m e^{-m}\left|e^{\theta(m)} - 1\right|}{\sqrt{2\pi m}m^m e^{-m}} = \left|e^{\theta(m)} - 1\right|. \tag{28}$$

Следует отметить, что $\left|\theta(m)\right| < \frac{1}{12m}$, где m – число, для которого вычисляется искомый факториал.

Проведем дальнейший анализ погрешности, связаной с вычислением по формуле (14). При выводе этой формулы было использовано приближение (10), однако значение $e^{\theta(m)} \le e^{\frac{1}{12m}}$ учтено не было. Если учесть данное значение приближения, то в формулах (11) могут появиться дополнительные множители ϑ_1 и ϑ_2, где

$$\vartheta_1 = e^{\frac{1}{12(L-Z+n-1)}}, \tag{29}$$

$$\vartheta_2 = e^{\frac{1}{12(L-Z)}}. \tag{30}$$

С учетом (23) и (24) формула (7) примет вид:

$$P'_{пш} = 1 - \exp\{-n+1\}\exp\{n-1\}\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}\frac{\vartheta_1}{\vartheta_2}. \quad (31)$$

Производя дальнейшие упрощения согласно методике вычисления (14), получаем:

$$\mathrm{P'_{пш}} = 1-\left[1-\frac{\mathrm{Z}}{\mathrm{L}}\right]^{(\mathrm{n}-1)}\left[1+\frac{\mathrm{n}-1}{\mathrm{L}-\mathrm{Z}}\right]^{(\mathrm{n}-\frac{1}{2})} exp\left(\frac{1}{12(\mathrm{L}-\mathrm{Z}+\mathrm{n}-1-\mathrm{L}+\mathrm{Z})}\right) =$$

$$= 1-\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}\exp\left(\frac{1}{12(n-1)}\right) \quad (32)$$

Проанализируем (32). Очевидно, что погрешность можно найти и для $P_{пш}$ совместно с $P^{l}_{пш}$ аналогично (28). Тогда, применив (25), получим:

$$\delta(a) = \left|\frac{1-\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}\exp\left(\frac{1}{12(n-1)}\right)-1-\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}}{1-\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}}\right| =$$

$$= \left|1-\exp\left(\frac{1}{12(n-1)}\right)\right|. \quad (33)$$

Теперь, сравнив (28) и (33), можно сделать вывод о равенстве оценок погрешности.

Далее сделаем оценку погрешности, допущенной при получении (14). Во-первых, погрешность обусловлена применением бинома Ньютона для аппроксимированного значения аргумента и асимптотического приближения $\lim_{x\to\infty}(1-\frac{\gamma}{x})^x = e^{\gamma}$, которое использовано при переходе от выражения (13) к (14). Во-вторых, поскольку в выражении (13) присутствуют разные значения x, то значение погрешности, которое дают формулы (13) и (14), не может быть, очевидно, оценено относительно $\lim_{x\to\infty}(1-\frac{\gamma}{x})^x = e^{\gamma}$.

Тогда очевидной будет попытка оценки погрешностей, которые дает формула (14) относительно предварительно упрощенной точной эталонной формулы (16). Для подсчета обозначим значение, которое дает формула (14) как $P^{l}_{пш}$. Тогда с использованием формулы (19) можем получить дополнительную оценку погрешности для формулы (14):

$$\delta(P'_{пш}) = \left|\frac{1-\left[1-\frac{Z-n+1}{L}\right]\left[1-\frac{Z-n+2}{L}\right]\ldots\left[1-\frac{Z+1}{L}\right]-1-\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}}{1-\left[1-\frac{Z}{L}\right]^{(n-1)}\left[1+\frac{n-1}{L-Z}\right]^{(n-\frac{1}{2})}}\right|. \quad (35)$$

Очевидно, что определение погрешности согласно данной формуле может быть произведено только с применением ЭВМ.

Так абсолютная погрешность для выборки 2^{16} сообщений при их длине в 10^8 бит, рассчитанная согласно формуле (35) при различных значениях длины сгенерированной последовательности, приведена в табл. 1, значения L и N, при которых были вычислены погрешности, приведены в табл 2.

Таблица 1

L / n	2^{64}	2^{128}	2^{192}	2^{256}	2^{512}
2^{16}	1,04544E-06	5,77846E-26	3,132486E-45	1,698121E-64	1,466490E-141

Таблица 2

L / N	2^{64}	2^{128}	2^{192}	2^{256}	2^{512}
2^{16*}	2,3013757E-02	1,26215817E-21	6,8421731E-41	3,7091495E-60	3,203284E-137
2^{16**}	2,3014803E-02	1,26221596E-21	6,8424864E-41	3,7093193E-60	3,203430E-137
2^{32*}	1	5,42105208E-12	2,9387582E-31	1,5931040E-50	1,375831E-127
2^{32**}	1	н/д	н/д	н/д	н/д

* – значения, вычисленные по формуле (14)

** – значения, вычисленные для точной эталонной формулы (16).

При значениях $n \geq 2^{32}$ вычисление значения по эталонной формуле (16) стает затруднительным и примерно равно 609000 секунд для вычисления одного значения, что может быть приравнено к одной недели непрерывных вычислений.

IV Результаты вычислений

Приведенные ниже вычисления были проведены с использованием пакета для математических вычислений Scientific Work Place 3.0 TCI Software Research, а также с помощью программой реализации вычисления по эталонной формуле (16) с использованием библиотеки многократной точности M.I.R.A.C.L. версии 4.8.

Вероятности перекрытия шифра как функция от n и L для l_m = 1000/10000 и l_m = 100000/1000000 представлены в табл. 3 и табл. 4 соответственно.

Таблица 3 – Вероятности перекрытия шифра для l_m = 1000/10000

n / L	2^8		2^{16}		2^{32}		2^{64}	
	1000	10000	1000	10000	1000	10000	1000	10000
2^{32}	0,0151	0,141	1	1	1	1	1	1
2^{40}	5,93E-05	5,93E-04	1	1	1	1	1	1
2^{42}	1,48E-05	1,48E-04	0,623	0,99994	1	1	1	1
2^{46}	9,26E-07	9,28E-06	0,592	0,4568	1	1	1	1
2^{48}	2,31E-07	2,32E-06	0,1513	0,1415	1	1	1	1
2^{50}	5,79E-08	5,80E-07	3,80E-02	3,74E-02	1	1	1	1
2^{64}	3,53E-12	3,54E-11	2,33E-07	2,33E-06	1	1	1	1
2^{128}	1,92E-31	1,92E-30	1,26E-26	1,26E-25	5,42E-17	5,42E-16	1	1
2^{192}	1,04E-50	1,04E-49	6,84E-46	6,84E-45	2,93E-36	2,93E-35	5,42E-17	5,42E-16
2^{256}	5,63E-70	5,63E-69	3,73E-65	3,71E-64	1,59E-55	1,59E-54	2,94E-36	2,94E-35

Таблица 4 – Вероятности перекрытия шифра для l_m = 100000/1000000

n / L	2^8		2^{16}		2^{32}		2^{64}	
	100000	1000000	100000	1000000	100000	1000000	100000	1000000
2^{32}	0,782	1	1	1	1	1	1	1
2^{40}	5,92E-03	5,76E-02	1	1	1	1	1	1
2^{42}	1,48E-03	1,47E-02	1	1	1	1	1	1
2^{46}	9,28E-05	9,27E-04	0,998	1	1	1	1	1
2^{48}	2,32E-05	2,32E-04	0,783	1	1	1	1	1
2^{50}	5,80E-06	5,80E-05	0,317	0,978	1	1	1	1
2^{64}	4,10E-10	3,5E-09	2,33E-05	2,33E-04	1	1	1	1
2^{128}	1,92E-29	1,92E-28	1,26E-24	1,26E-23	5,42E-15	5,42E-14	1	1
2^{192}	1,04E-48	1,04E-47	6,8E-44	6,8E-43	2,93E-34	2,93E-33	5,42E-15	5,42E-14
2^{256}	5,63E-68	5,64E-67	3,71E-63	3,71E-62	1,59E-53	1,59E-52	2,94E-34	2,94E-33

V Заключение

В работе сформулирована и решена задача расчета и обоснования срока действия ключей поточного шифра или блочного шифра, используемого в режиме гаммирования.

Данная задача является сложной и противоречивой и включает в себя построение оценок различных параметров, характеризующих так называемое явление перекрытия отрезков последовательности, соответствующих заданным различным значениям вектора инициализации. Одной из наиболее важных для последующих исследований в этом направлении является задача оценки (в зависимости от шифрующего преобразования) допустимой суммарной длины отрезков сгенерированной последовательности, при которой эффектом их перекрытия можно пренебречь. Данная задача частично рассмотрена в [5]. Также было определено, что алгоритмы такого класса безопасны при использовании стандартных длин ключа более 128 бит.

Следует отметить, что изложенные результаты вероятностного анализа перекрытий отрезков последовательностей могут быть непосредственно применены при расчете сроков действия ключей поточных и блочных шифров, используемых в режиме счетчика.

Литература: ***1.*** *Харин Ю. С., Берник В. И., Матвеев Г. В. Математические основы криптологии. – Минск: Изд-во БГУ, 1999. – 319 с.* ***2.*** *Колчин В. Ф., Севастьянов Б. А., Чистяков В. П. Случайные размещения. – М.: Наука, 1976. – 223 с.* ***3.*** *Михайлов В. Г. О повторяемости состояний датчика псевдослучайных чисел при его многократном использовании // Теория вероятности и ее применение – 1995. – Т. 40. – Вып. 4. – С. 786 – 797.* ***4.*** *Левин Б. Р. Теоретические основы статистической радиотехники. Книга первая. Изд. 2-е, перераб. и доп., М., «Сов. Радио», 1974, 552 с.* ***5.*** *Коваленко И. Н., Левитская А. А., Савчук М. Н. Избранные задачи вероятностной комбинаторики. – К.: Наукова думка, 1986. – 224 с.* ***6.*** *Малая советская энциклопедия, под ред. Б. А. Введенского, т. 7, изд, 3-е, 1959 г.*

УДК 681.3.06:519.248.681

МЕТОД ФОРМИРОВАНИЯ ЦИКЛОВЫХ ПОДКЛЮЧЕЙ НА БАЗЕ ЛИНЕЙНЫХ РЕГИСТРОВ СДВИГА В РАСШИРЕННЫХ ПОЛЯХ GF (2^N)

Александр Лепеха

Харьковский национальный университет радиоэлектроники

Анотація: **Сформульовані вимоги до сучасних схем розгортання ключів. Розглядається метод побудови схеми розгортання на базі лінійних регістрів зсуву в розширених полях GF(2^n). Приводиться порівняльний аналіз із аналогічними конструкціями.**

Summary: **In this article are presented requirements to modern key schedules. The method of construction of the circuit of deployment is considered on the basis of linear registers of shift in the expanded fields GF(2^n). The comparative analysis with similar designs is carried out.**

Ключові слова: **Схема розгортання ключів, генератор псевдовипадкових послідовностей, лінійні регістри зсуву.**

Введение

При оценке криптографической стойкости блочного симметричного шифра (БСШ) большое внимание уделяется способности шифра противостоять наиболее мощным на сегодняшний день методам линейного и дифференциального криптоанализа. В связи с этим большинство работ посвящены совершенствованию указанных методов криптоанализа либо улучшению криптографических свойств цикловой функции шифра. Однако в последнее десятилетие получили развитие методы криптоанализа, которые используют особенности формирования цикловых подключей схемами разворачивания ключей. Проведенный автором обзор современных БСШ, представленных в проекте NESSIE [1], показал, что многие криптографические алгоритмы, обладающие цикловой функцией, способной противостоять атакам на основе линейного и дифференциального криптоанализов, оказываются уязвимыми к атакам на схемы разворачивания ключей. Примером могут служить 3-DES, IDEA, SAFER (SAFER+), Hierocrypt, Noekeon. Для других алгоритмов использование атак на схему разворачивания ключей оказалось более эффективно по сравнению с классическими методами криптоанализа. Например, для БСШ Rijndael одним из недостатков, указанных при проведении конкурса NESSIE, является низкая граница безопасности (запас 2 цикла для версии алгоритма с